DEPARTMENT OF HEALTH AND HUMAN SERVICES
Public Health Service
Indian Health Service
Rockville, Maryland 20857 Refer to: OIRM/SPSS

INDIAN HEALTH SERVICE CIRCULAR NO. 93-06

AUTOMATED INFORMATION SYSTEMS SECURITY PROGRAM

Sec.

1. Purpose
2. Background
3. Scope
4. Policy
5. Procedures
6. Responsibilities
7. Definitions
8. References
9. Supersession

1. PURPOSE. This circular establishes Indian Health Service (IHS) policies, procedures, and responsibilities for the implementation and administration of an Automated Information Systems (AIS) Security Program.

2. BACKGROUND. The Computer Security Act of 1987 requires Federal agencies to identify computer systems that contain sensitive information, to establish a plan for the security and privacy of these systems, and to provide computer security awareness training. In addition, Federal agencies must comply with regulatory requirements such as:

   A. Office of Management and Budget (OMB) Circular No. A-130, Management of Federal Information Resources, as amended, which requires Federal agencies to implement and maintain an AIS security program, including the preparation of policies, procedures, and standards. This program includes four primary elements: applications security, personnel security, information technology installation security, and security awareness and training;

   B. OMB security bulletins which annually provide guidance to Federal agencies regarding computer security requirements; e.g., OMB Bulletins 90-08, 91-10, and 92-05, provide instructions for preparing system security plans and annual reporting;

Distribution: PSD 557 (Indian Health Mailing Key)
Date: September 10, 1993

C. Department of Health and Human Services (DHHS) AIS Security Program Handbook, as amended, which provides security program implementation instructions to the agencies within the Department;

D. DHHS AIS Security Training and Orientation Program (A-STOP) Guide, as amended, which was developed to ensure that all employees receive appropriate computer security training;

E. DHHS Information Resources Management (IRM) CIRCULAR #lO which established policies, procedures, and responsibilities for the implementation and administration of a Departmental security program for AIS; and

F. Public Health Service's (PHS) IRM Manual PART 6 - Automated, Information Systems Security, as amended.

A more extensive listing of references is included in Section 8.

3. SCOPE. This circular applies to all INS, contractors (Public Law (P.L.) 93-638), state, and local organizations performing IHS functions.

4. POLICY. The AIS Security Program will ensure that each AIS has a level of security that is cost-effective and is commensurate with the risk and magnitude of harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security must protect the integrity, confidentiality, and availability of the information and is required to have:

A. The appropriate technical, personnel, administrative, environmental, and telecommunications safeguards; and

B. A contingency or disaster recovery plan to provide continuity of operation for AISs which support critical agency functions.

5. PROCEDURES.

A. The DHHS AIS Security Program Handbook, as amended, contains security procedures and instructions for IHS Area Offices and Headquarters (AO/HQ).

B. The DHHS A-STOP Guide, as amended, contains procedural guidance for implementing security awareness and training.

c. Guidance will be developed specific to the IHS on security training and procedures for all Information Systems Security Officers (ISSOs) and end-users.

6. RESPONSIBILITIES.

A. The Director, IHS, oversees the IHS AIS Security Program and is responsible for approving related directives.

B. The Associate Director, Office of Information Resources Management, is the Designated Approving Authority for the AIS Security Program and is responsible for:

(1) Managing the program in accordance with statutory and regulatory requirements; and

(2) Appointing the IHS, Headquarters East (HQE) and Headquarters West (HQW) ISSOs.

c. The IHS ISSO is responsible for the development and implementation of the AIS Security Program to protect the Agency's AIS resources and will:

(1) Promote and coordinate Agency-wide AIS Security Program activities to ensure consistency, cost-effectiveness, and comprehensiveness;

(2) Act as liaison to other Agencies regarding AIS security functions;

(3) Monitor Area Office activities by:

a. Reviewing annual Area Office security plans for compliance with IHS and Federal regulations;
b. Reviewing security status reports; and
c. Evaluating safeguards used to protect major AISs.

(4) Conduct IRM reviews of the Area Offices and Headquarters to ensure conformance with IHS and Federal AIS security policies; and

(5) Provide security guidance, training and assistance to the Area Office and Headquarters ISSOs.

D. Area Directors are responsible for implementing the AIS Security Program and shall appoint Area Office (AO) ISSOs to assist in the coordination and implementation of the program. No ISSO shall have duties which create a conflict of interest.

E. The AO/HQE/HQW ISSOs will implement security policies, procedures, standards, and guidance consistent with IHS requirements. Responsibilities include:

(1) Implement a program to incorporate appropriate administrative, physical, and technical safeguards into all new applications and into significant modifications to existing applications as required by OMB Circular A-130, Appendix III, as amended;

(2) Implement and maintain Computer Systems Security Plans to fully comply with the Computer Security Act of 1987 and OMB Bulletins;

(3) Submit annual AIS Security Plan to the IHS ISSO for review and comment;

(4) Review and validate Agency Procurement Requests for the inclusion of all AIS security requirements and safeguards per current OMB A-130 and Federal Information Resources Management Regulations (FIRMR) Chapter 201;

(5) Fulfill security awareness and risk management training needs per the Computer Security Act of 1987, National Institutes for Science and Technology (NIST) Special Pub 500-172, and DHHS AIS Security Program Handbook Chapter VII, as amended;

('5) Verify with their Personnel Office that AIS personnel have suitability per the current Federal Personnel Manual (FPM) Chapter 731 and DHHS Instruction 731-1, Personnel Security and Suitability Policy and Technical Guidance;

(7) Certify, with recertification every three years, the observation/inclusion of security safeguards for sensitive systems, and accredit same, per amended OMB Circular A-130, Appendix III, Federal Information Processing Standards (FIPS) Pub. 102; and DHHS AIS Security Program Handbook Chapter IX, as amended; and

(8) Ensure 'that personnel assigned major information system responsibilities are properly trained per NIST Special Pub 500-172 and DHHS A-STOP Guide, as amended.

7. DEFINITIONS.

A. AIS An electronically based system for the organized collection, processing, transmission, and dissemination of information in accordance with defined procedures. (Reference: OMB Circular A-130).

B. Accreditation. The authorization and approval, granted to an AIS system or network to process sensitive data in an operational environment and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. (Reference: FIPS Pub 102).

C. Certification. A technical evaluation made as part of, and in support of, the accreditation process, that establishes the extent to which *a* particular computer system or network design and implementation meet a pre-specified set of security requirements. (Reference: FIPS Pub 102).

D. Computer security. The quality exhibited by a computer system that embodies its protection against internal failures, human errors, attacks, and natural catastrophes that might cause improper disclosure, modification, destruction, or denial of service. *(Reference:* FIPS Pub 102).

E. Computer system security plan. A document describing the security and privacy requirements of a given system and the agency's plan to meet these requirements. (Reference: OMB Bulletin No. 90-08).

F. Designated Approving Authority (DAA). The Official who has the authority to decide on accepting the security safeguards prescribed for an AIS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

G. IHS ISSO. The Agency representative responsible to the DAA for the policy, planning, coordination, and overall guidance of the IHS AIS Security Program.

H. TSSO (Area Office and Headquarters). The person responsible for ensuring that security is provided for and implemented throughout the life cycle of an AIS this includes: initial concept, planning, design, development, operation, maintenance, and secure disposal.

I. Major information system. An information system that requires special continuing management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant impact on the administration of agency programs, finances, property, or other resources. (Reference: OMB A-130).

J. Sensitive information. Any information the loss, misuse, or unauthorized modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act. DHHS AIS Security Program Handbook Chapter II provides additional guidance on how to determine the appropriate security levels for sensitive information. (Reference: Computer Security Act of 1987).

8. REFERENCES.

A. Computer Security Act of 1987 (P.L. 100-235)
B. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, Security of Federal Automated Information Systems (AIS)
C. OMB Circular No. A-123, Internal Control Systems
D. OMB Circular No. A-127, Financial Management Systems
E. OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
F. Federal Personnel Manual (FPM), Chapter 731, Personnel Suitability
G. FPM Department of Health and Human Services (DHHS) Instruction 731-1, Personnel Security/Suitability Policy and Technical Guidance
H. DHHS AIS Security Program
I. DHHS AIS Security Training and Orientation Program Guide
J. National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS Pub) 31 Guideline for Automated Data Processing (ADP) Physical Security and Risk Management
K. FIPS Pub 65 Guideline for ADP Risk Analysis

L. FIPS Pub 73 Guideline for Security of Computer Applications
M. FIPS Pub 87 Guideline for ADP Contingency Planning
N. FIPS Pub 102 Guideline for Computer Security Certification and Accreditation
0. NIST-Special-Pub-500-169, Executive Guide to the Proteotion of Information Resources
P. NIST Special Pub 500-170, Management Guide to the Protection of Information ***Besources***
Q. NIST Special Pub 500-171, Computer User's Guide to the Protection of Information Resources
B. NIST Special Pub 500-172, Computer Security Training Guidelines
S. General Services Administration Federal Information **Besources** Management Regulations Chapter 201

9. SUPERSESSION.

None.

Michel E. Lincoln
Acting Director, Indian Health Service